# Securing and Compressing Files

# for Electronic Transmission

# User Guide

**18 January 2002**

**Edition 1.0**

**Patient Administration Systems and Biostatistics Activity (PASBA)**

**1216 Stanley Road**

**Fort Sam Houston, Texas 78234-6053**

**Contents**

**Figures**

# 1 Introduction

This document provides recommended guidance and reference information on securing and compressing files for electronic transmission. This guide is intended for U.S. Army Medical Command (MEDCOM) patient administrators and information management personnel responsible for sending and receiving data deemed sensitive but unclassified (SBU) during deployment.

# 2 Recommendation for Securing Data Transmissions

The Patient Administration Systems and Biostatistics Activity (PASBA) strongly encourages the use of the Pretty Good Privacy (PGP) software for securing the electronic transmissions of all sensitive but unclassified (SBU) data. Data considered SBU includes:

- all data protected under the U.S. Privacy Act of 1974
- all population and location data associated with areas of operations
- any data item that identifies an individual by name, Social Security Number, hospital register number, diagnosis, and so forth.

## 2.1 PGP Software

Pretty Good Privacy (PGP) software is a freeware product suite "that enables people to securely exchange messages, and to secure files, disk volumes and network connections with both *privacy* and *strong authentication*. *Privacy* means that only the intended recipient of a message can read it. By providing the ability to encrypt messages, PGP provides protection against anyone eavesdropping on the network. Even if the information is intercepted, it is completely unreadable to the snooper. *Authentication* identifies the origin of the information, certainty that it is authentic, and that it has not been altered. Authentication also provides an extremely valuable tool in network security: verification of the identity of an individual." [1]

---

[1] MIT website: http://web.mit.edu/network/pgp.html

## 2.2  Downloading and Installing PGP

Since the PGP software should not be downloaded from locations outside the U.S. or Canada, PASBA recommends downloading the PGP software prior to deployment. If you are unable to download PGP, contact PASBA for assistance.

The PGP software is available for several different operating systems including Windows 95/98/NT/2000 and the Macintosh. There is no cost for personal, non-commercial use of PGP.

To download the PGP program, go to the MIT website at http://web.mit.edu/network/pgp.html and click the Download link for your platform. Respond to the prompts to download the software to your location. To install the software, simply accept the default values presented by the installation program.

## 2.3  Using PGP

A comprehensive set of user documentation is included with the PGP software. In addition to installation instructions, the documentation describes how to use PGP to encrypt files, decrypt files, and set-up an interface with Microsoft Outlook.

### 2.3.1  Process Summary

The following section summarizes the process for encrypting and signing files after you've installed PGP:

1. Create a private and public key pair. A PGP key pair is composed of a private key to which only you have access and a public key that you can copy and make freely available to everyone with whom you exchange information. See "Making a Key Pair" in the *PGP User Guide*.
2. Exchange public keys with others.
3. Validate public keys.
4. Encrypt and sign your e-mail and files. There are several ways to encrypt and sign files with PGP:
   - From the System tray (PGPtray)

- From within supported e-mail applications (Microsoft Outlook)
- From PGPtools
- From the Windows Explorer File menu

### 2.3.2  Sample Procedure: Encrypting Files

The following procedure shows how to encrypt a file from Windows Explorer. For a detailed explanation on any feature in PGP, refer to the PGP user documentation provided with the PGP software.

After installing PGP, perform the following procedure to encrypt a file that you want to e-mail:

1.  Open Explorer and go to the disk location of the file you want to encrypt and send.

2.  From Windows Explorer, right-click on the file. From the pull-down menu, select PGP then select the Encrypt command. See Figure 1.
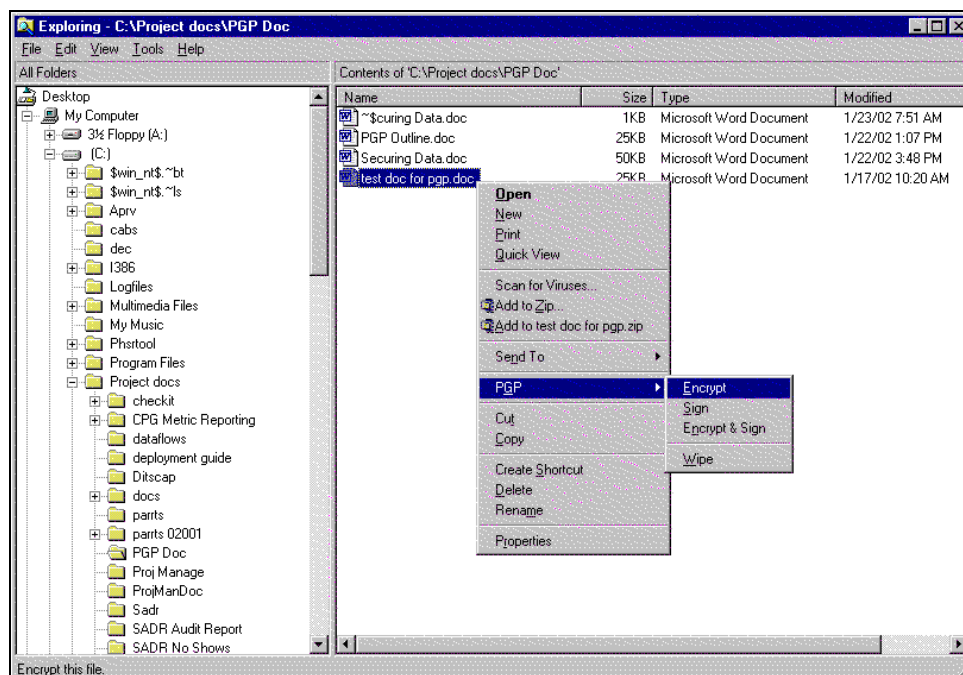


**Figure 1. Select Encrypt Command**

3.  From the Key Selection Dialog box, select the Conventional Encryption and Self-Decrypting Archive options (see Figure 2). These options allow you to create an

encrypted, executable file and send it to recipients that may or may not have PGP installed.



Select these options.
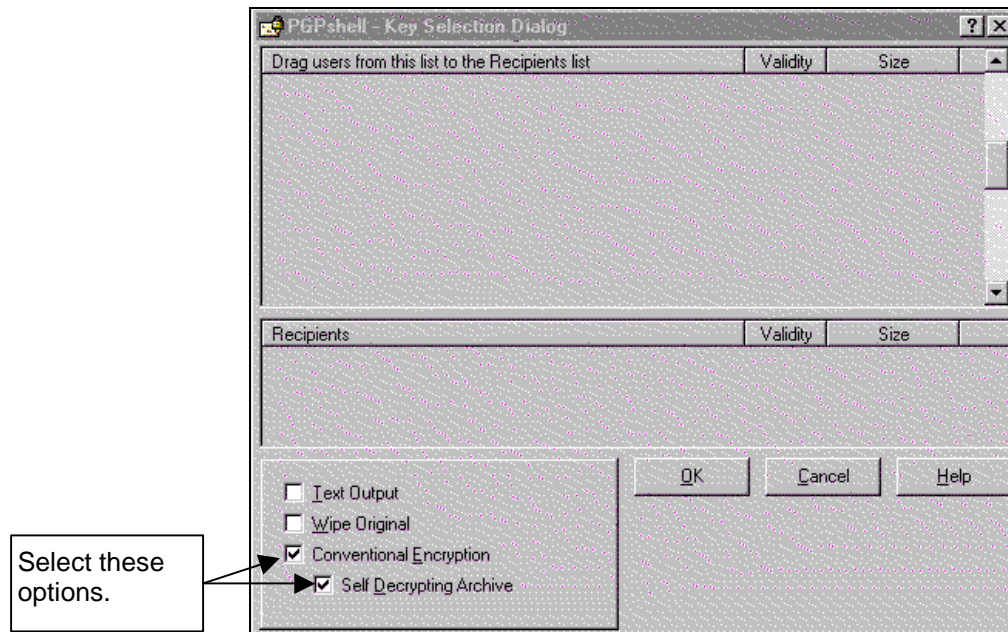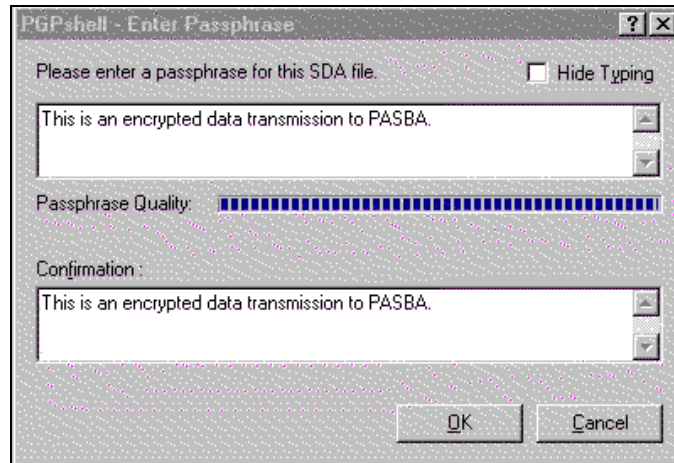
**Figure 2. Select Encrypting Options**

4.    From the Key Selection Dialog box, select OK. The Enter Passphrase window displays. See Figure 3.
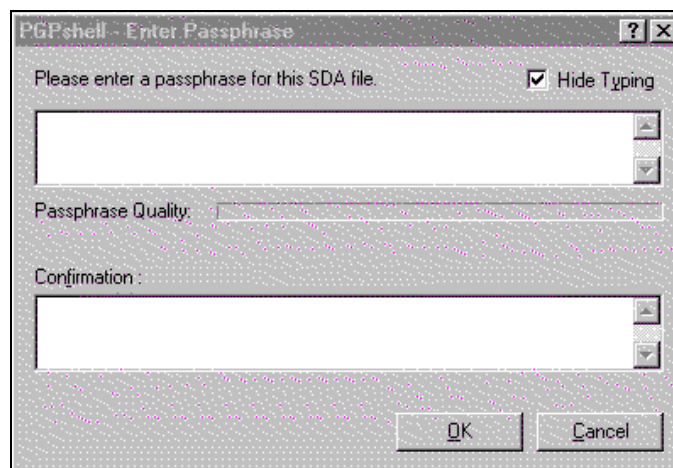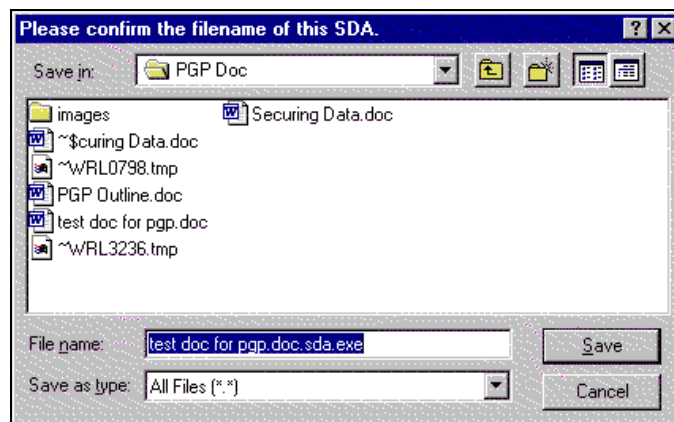


**Figure 3. Enter Passphrase**

5.    From the Enter Passphrase window, type your passphrase for this file. Then type the passphrase again in the Confirmation section of the window. Note that the passphrase text is case sensitive. See Figure 4.

**Figure 4. Passphrase Dialog Box**

6.    From the Enter Passphrase window, click OK. The file save dialog box displays:



**Figure 5. Save Encrypted File**

7.    From the file save dialog box (see Figure 5), click the OK button to save the
      encrypted file. Optionally, you can select a different disk location and type a new
      name for the encrypted file. However, this author recommends using the default
      file name and location.

8.    Click Save to save and encrypt the file. The encrypted file is saved with an
      .sda.exe extension (sda.exe is appended to the end of the filename).

9.    Open your e-mail program, select the recipient(s) for your message, and attach
      the encrypted file with the message. You must also send the passphrase to the
      recipient(s) so that the file can be decrypted when the message is received. You
      may want to telephone the recipients to give them the passphrase or send the

passphrase in a separate message. The recipient is prompted for the passphrase when they attempt to open the file.

### 2.3.3  Decrypting Files

When you receive an email message or file that has been encrypted, you must decrypt the message or file to make sure that the data originated with the alleged sender and that it has not been altered. The passphrase must be typed exactly as it was entered. Remember, the passphrase text is case sensitive.

### 2.3.4  PGP User Documentation

The user documentation supplied with the PGP software describes how to use all of the features of the software. Always refer to the PGP documentation for detailed information on encrypting and decrypting files and messages.

# 3  Using Compression Software

When sending large files via e-mail, PASBA recommends the use of compression software to reduce the size of large files and expedite the transmission of the files. ZipCentral is one type of data compression software that offers a simple interface for compressing and managing zip files. The ZipCentral software can be downloaded for free from the Internet.

## 3.1  Downloading ZipCentral

To download the ZipCentral software:

1.      Open your web browser and go to http://zipcentral.iscool.net.
2.      From the ZipCentral website home page, click the Download link in the upper, right corner of the window. The download window displays.
3.      Select the language from the pull down menu. Another window displays.
4.      Select the download site from the choices presented.
5.      Click the Save button to save the installation file to your PC. The system displays a message when the download is complete.

### 3.1.1  Installing ZipCentral

To install ZipCentral on your PC:

1.  After the file is downloaded and saved on your PC, open Windows Explorer and go to the location where you saved the ZipCentral installation file.
2.  From Windows Explorer, double-click the ZipCentral installation file.
3.  Follow the installation prompts to install the software on your PC. In most situations, you should accept the default values presented during the installation process.

## 3.2  Using ZipCentral

The ZipCentral software comes with on-line user documentation that describes in detail how to use the ZipCentral software. The following section summarizes the basic steps for compressing and uncompressing files using ZipCentral. As a general rule, any file over 1 megabyte (1 Mb) that you intend to e-mail should be compressed.

When you're ready to zip up a file or group of files, perform the following procedure:

1.  Open the ZipCentral program by selecting the command from the Windows Start menu or by clicking the ZipCentral icon on your Windows desktop. The ZipCentral program opens (see Figure 6).
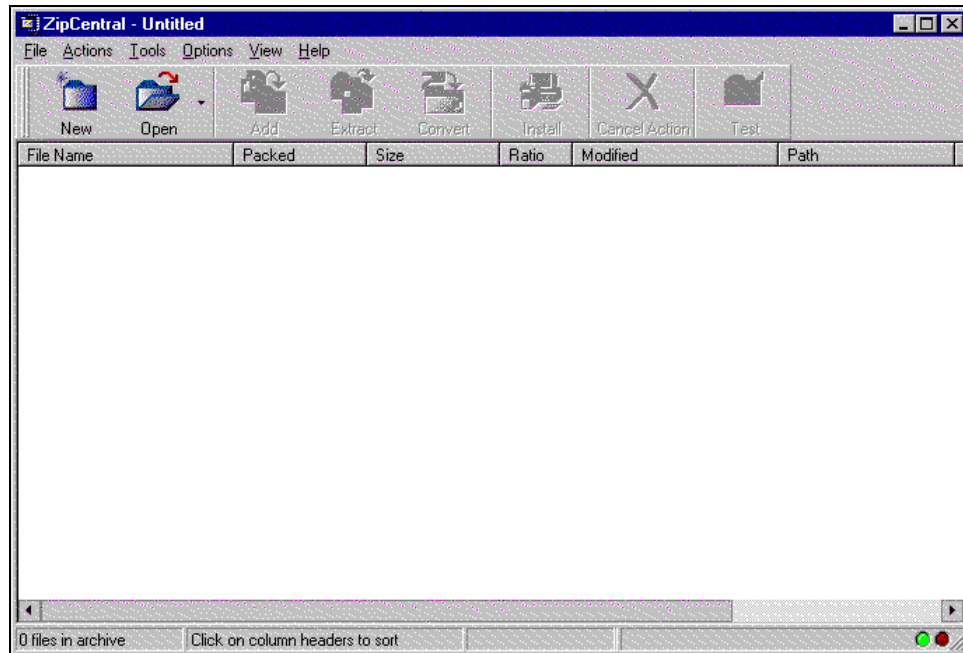
**Figure 6. ZipCentral Main Window**

2.    From the ZipCentral main window, click the New command at the top of the window or select New Archive from the File menu. The program prompts for a name for the zip file. The zip file contains the file or files you want to compress.
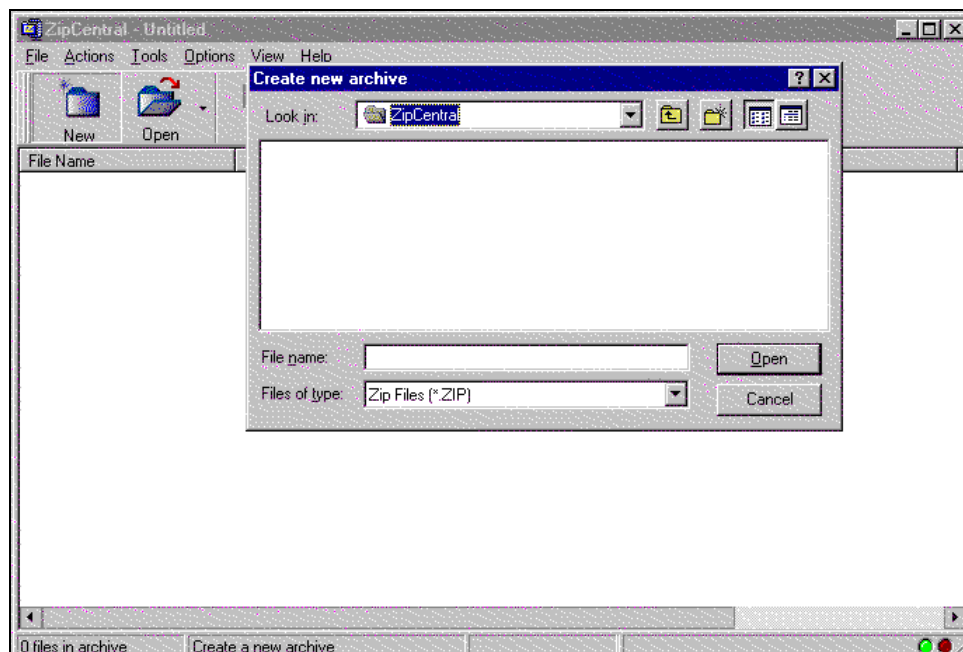


**Figure 7. Create New Archive Dialog Box**

3.   Type the name of the zip file in the File Name field. Optionally, select the location where you want to store the file.

4.   From the Create new Archive window, click the Open button. The program displays a window from which you can select the file(s) you want to copy into the zip file.
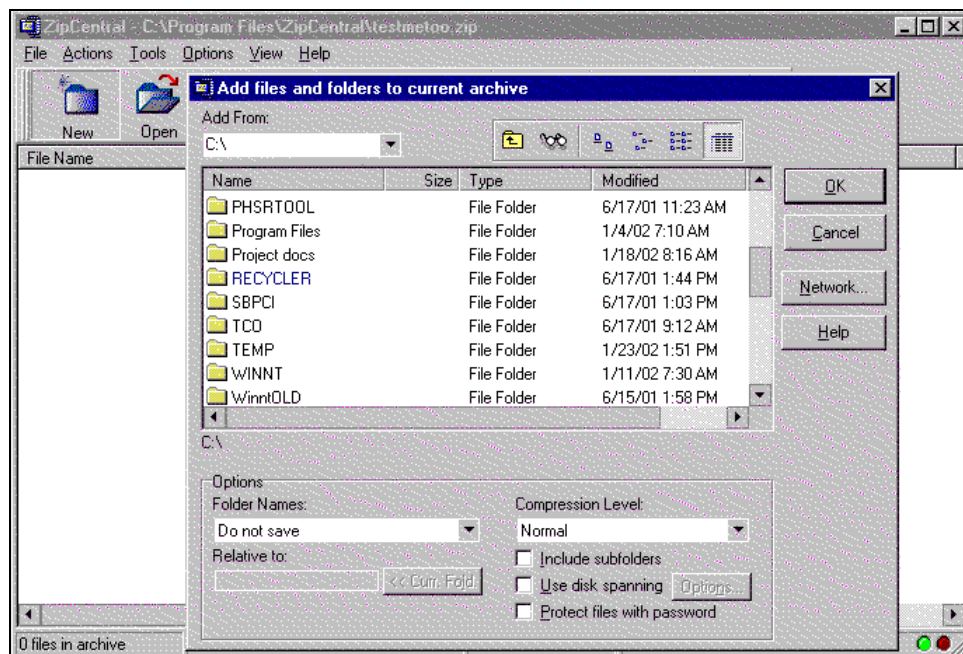


**Figure 8. Select Files for Zip File**

5.   Navigate to the disk location of the file(s) you want to copy into the zip file you created in step 3 and click OK. Repeat this step for each file you want to copy to the zip file. If necessary, you can return to the main window and use the Add command to copy additional files into the zip file.

6.   To zip the file, choose Convert to executable from the Tools menu or click the Convert button at the top of the ZipCentral main window. The Create self extracting archive window displays.

7.   From the Create self extracting archive window, set the options for this zip file and click OK. A self-extracting file (.exe) containing the selected files is created with the name and in the location you specified in step 3.

8. Choose Convert to executable from the Tools menu or click the Convert button to convert the self-extracting file to a zip file with the name and in the location you specified in step 3.

### 3.2.1 Extracting a Zip File

To unzip a compressed file using ZipCentral:

1. Open the ZipCentral program.
2. From the ZipCentral main window, choose Open Archive from the file menu or click the Open button. The Open Existing Archive dialog box displays.
3. Navigate to the location where the .zip file resides and double-click it.
4. From the Open existing archive window, click the Open button.
5. Choose the Extract command from the Actions menu or click the Extract button. The files in the zip file are extracted in the location you selected.

### 3.2.2 ZipCentral User Documentation

Refer to the Help file in the ZipCentral program for detailed instructions on using the software. To view the Help file, choose the Help menu option on the ZipCentral main screen.

## 4 References

- Download the PGP software from: http://web.mit.edu/network/pgp.html

- Download the ZipCentral software from: http://zipcentral.iscool.net

- View the PASBA website at: http://www.pasba.amedd.army.mil